2020 DOE Vehicle Technologies Office Annual Merit Review

Enabling Secure and Resilient XFC: A Software/Hardware-Security Co-Design Approach

Ryan M. Gerdes
Virginia Tech

June 4, 2020
Project ID elt207

This presentation does not contain any proprietary, confidential, or otherwise restricted information

Overview

Timeline

- 2018-10-01
- 2021-06-30
- Percent Complete: 55% (Q1, 2020)

Barriers

- Compromise is difficult to detect, contain, and mitigate
- Remote remediation of compromise
- Maintaining operational capacity under compromise

Budget

- Total project funding
  - $2,500,000 DOE funding
  - $625,000 cost share

Partners

- Academic: *Virginia Tech*, Georgia Tech, Utah State University
- Industry: Commonwealth Edison Company, Ford Motor Co., GE Research, Tritium

Relevance

- ***Enable the decrease in battery charge time in a secure and efficient manner***
  - coordination and cooperation between the grid, charging stations, and the vehicles
  - electric vehicle service equipment (EVSE) and the BEV themselves are untrustworthy

- **Resilient (and not just secure) system be put in place**
  - compromises of either BEV or EVSE are inevitable
  - maintain some operational capacity while guaranteeing safety

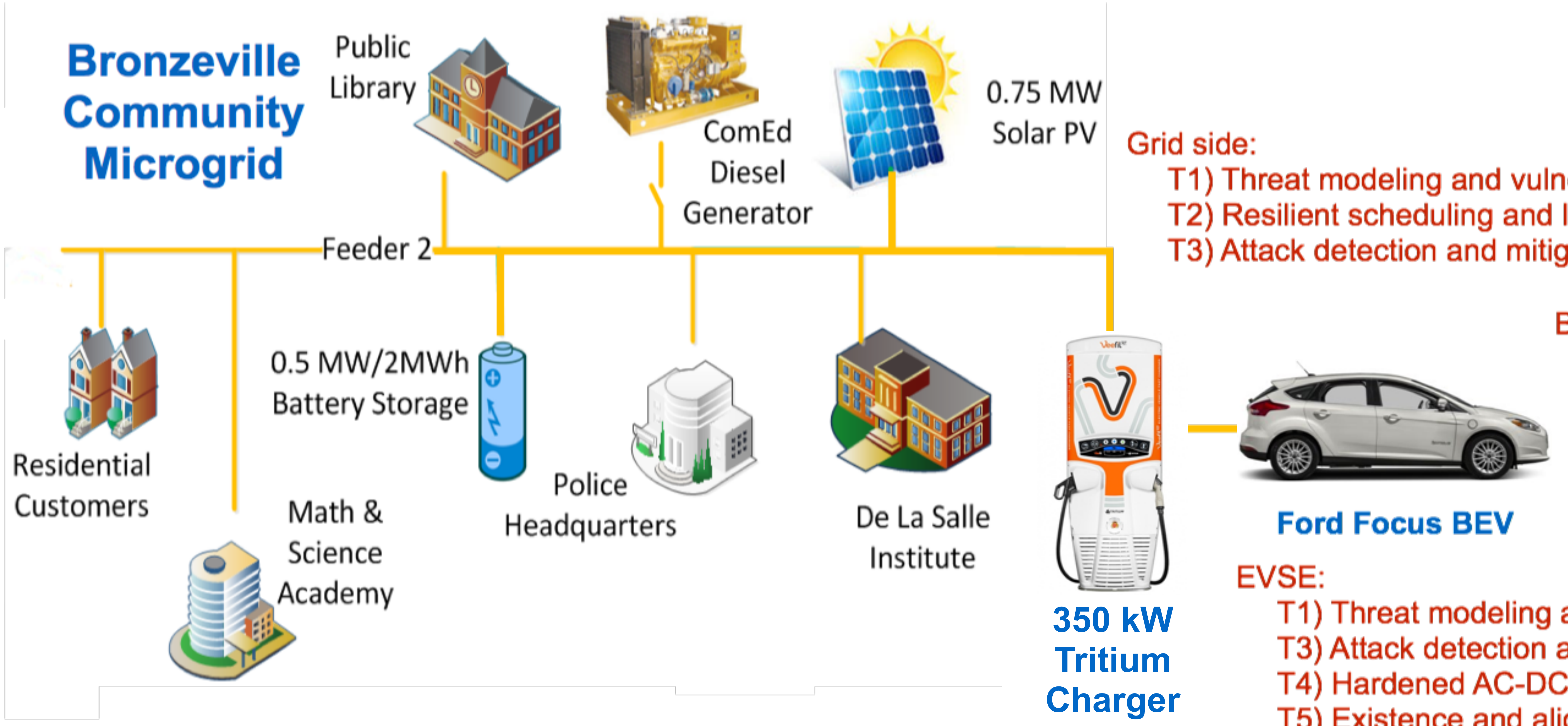
- **Motivating threats:**
  - A network of compromised EVSE could be used to simultaneously discharge the batteries of BEV
  - Compromised BEV, with possible collusion from compromised EVSE, drawing from the grid in a coordinated manner so as to cause instability
  - Malware being spread from a BEV to other BEV through the compromise of single or multiple EVSE

Approach

- **State-of-the-Art**
  - design process used for safety critical systems does not produce inherently more secure systems (e.g., automotive systems)
  - proprietary and/or high-level requirements
  - cyber-centric best practices lack cyber-physical systems security perspective

- **Hardware/software-security (HW/SW-Sec) co-design approach**
  - security-hardened controllers, converters, and monitoring systems: secure sensing/actuation techniques, moving-target based detection and mitigation strategies
  - guarantee successful remediation of vulnerabilities in EVSE/BEV through remote updates
  - respecting end-user privacy
  - conductive and inductive charging at power levels of 200 kW to 400

Approach



Grid side:
- T1) Threat modeling and vulnerability assessment
- T2) Resilient scheduling and load management
- T3) Attack detection and mitigation controller

BEV:
- T1) Threat modeling and vulnerability assessment
- T3) Attack detection and mitigation controller
- T4) Hardened DC-DC Converters and battery management
- T6) Secure updates
- T7) User privacy

EVSE:
- T1) Threat modeling and vulnerability assessment
- T3) Attack detection and mitigation controller
- T4) Hardened AC-DC Converters
- T5) Existence and alignment of BEV
- T6) Secure updates
- T7) User privacy

Approach: Milestones (FY2019-20)

Milestone	Type/Status	Description
Threat models (09/2019)	*Technical (Complete)*	*TARA report that lists the main threats to focus on later in the project*
Microgrid model (12/2019)	*Technical (Complete)*	*The model of Bronzville microgrid is developed in real-time simulators*
New designs for converter and BMS hardware (03/2020)	*Technical (Ongoing)*	*Critical design review completed with team and program manager approval of hardened designs*
MTD techniques with theoretical stability, optimality, and robustness guarantees (03/2020)	*Go/No-Go (Ongoing)*	*A proactive and reactive defense framework for the EVSE/BEV/grid controllers*

- **Hardware deployed:**
  - Ford Focus BEV (Blacksburg, VA)

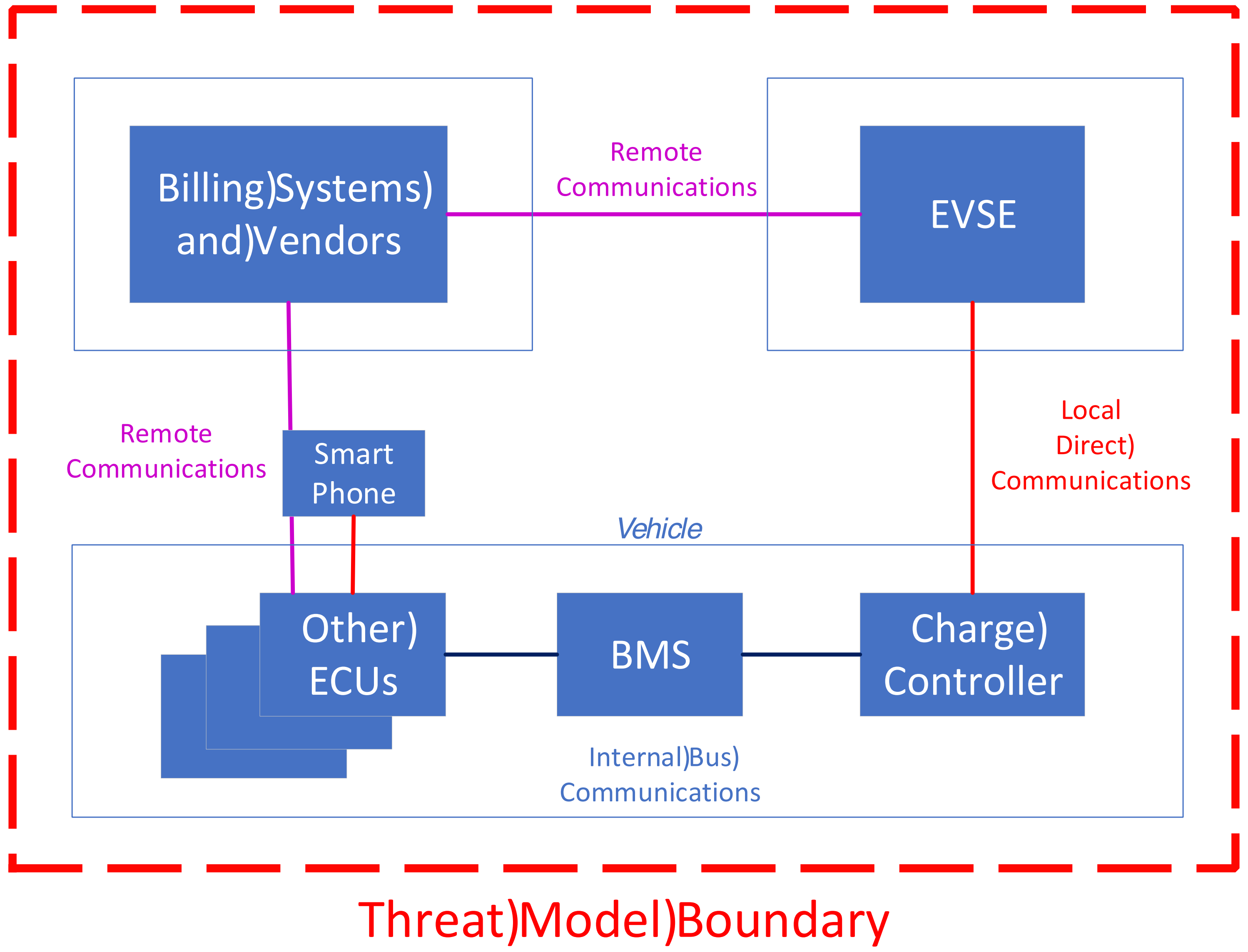
Approach: Milestones (FY2020)

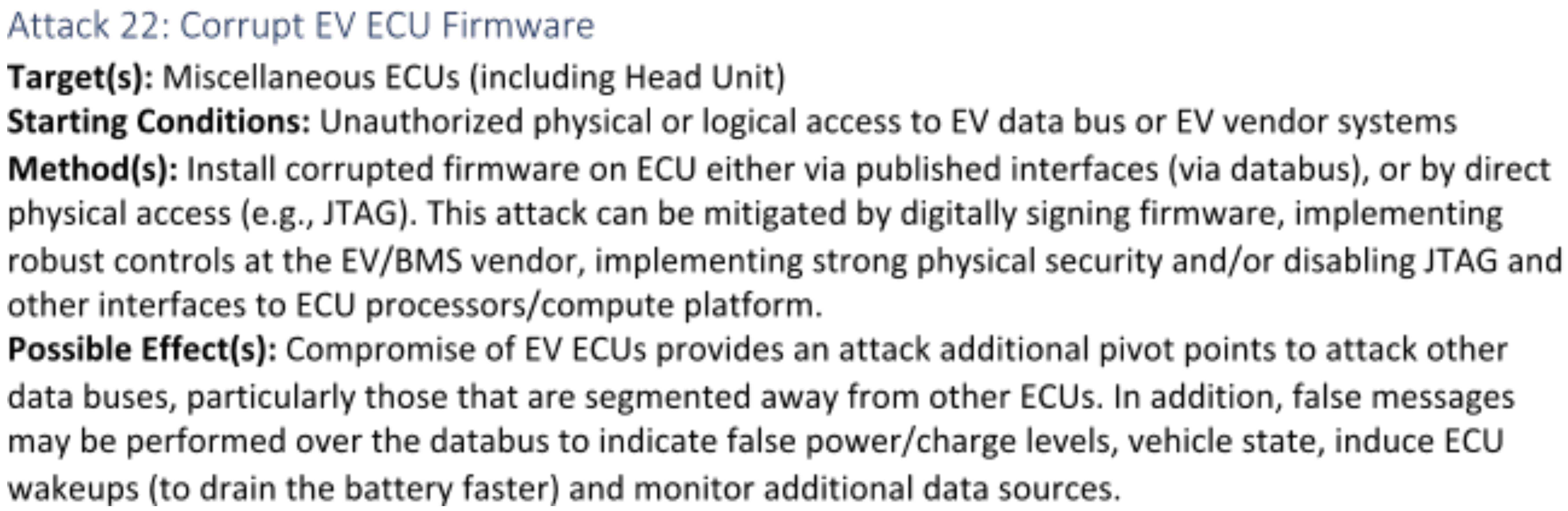
Milestone	Type	Description
Privacy Impact Assessment of EVSE/BEV communication (12/2020)	*Technical*	*Analyze data flows to identify personally identifiable information and ensure appropriate privacy controls*
Vulnerability assessment of EVSE/BEV-grid interactions (09/2020)	*Technical*	*Attack trees and attack graphs.*
Trade-offs of grid-side resiliency approaches (12/2020)	*Technical*	*Trade-offs for BEV-induced attacks are quantified*
Install and demonstrate the technology within the Bronzeville Community Microgrid (03/2021)	*Go/No-Go*	*Successful field demonstration given the minimum negative impact during the planning study*

- **Hardware to be deployed:**
  - USU XFC (conductive & inductive) bus (Logan, UT)
  - Tritium XFC charger (Q2, 2020, Chicago, IL)
  - Ford Focus BEV (Q2, 2020, VA)

Technical Accomplishments and Progress: T1

- **Threat assessment of EVSE/BEV/grid using TARA methodology**
  - BEV/EVSE assessment complete
    - 6 threats, 4 attack points, 27 attacks
  - EVSE/grid assessment to be completed upon integration of EVSE into research lab (Q3, 2020)
  - Participation in NMFTA XFC Cybersecurity Working Sub-Group A
  - Deliverable: *Electric Vehicle Charging Threats*, Internal, 2019
  - Insights:
    - Susceptible attack points identified (vulnerability assessment of vehicle to focus on EVSE/BEV communication using fuzzing)
    - Attacker can pivot from EVSE communication ECU to attack vehicle





Attack 22: Corrupt EV ECU Firmware

Target(s): Miscellaneous ECUs (including Head Unit)

Starting Conditions: Unauthorized physical or logical access to EV data bus or EV vendor systems

Method(s): Install corrupted firmware on ECU either via published interfaces (via databus), or by direct physical access (e.g., JTAG). This attack can be mitigated by digitally signing firmware, implementing robust controls at the EV/BMS vendor, implementing strong physical security and/or disabling JTAG and other interfaces to ECU processors/compute platform.

Possible Effect(s): Compromise of EV ECUs provides an attack additional pivot points to attack other data buses, particularly those that are segmented away from other ECUs. In addition, false messages may be performed over the databus to indicate false power/charge levels, vehicle state, induce ECU wakeups (to drain the battery faster) and monitor additional data sources.

Technical Accomplishments and Progress: T2

- **Vulnerability assessment of a Ford BEV**
  - 18 attack vectors identified: Permanent disabling/degradation of vehicle and harm to occupants/persons nearby
  - Validation of two high-impact vectors
  - Diagnostics specification
    - Battery Power Sensor Module (BPSM) can be compromised
    - BPSM provides BECM with critical sensor data
    - Develop injector to control traffic to/from BPSM (emulate compromise)
  - Ten undergraduate researchers (four independent studies Q1–Q2, 2020)
  - Formal assessment undertaken by new partners (Q3, 2020)
  - Deliverable: Publication TBD
  - Insight: Authenticated sensor data (battery temperature and coolant flow) allows for (possible) overheating of battery leading to thermal runaway

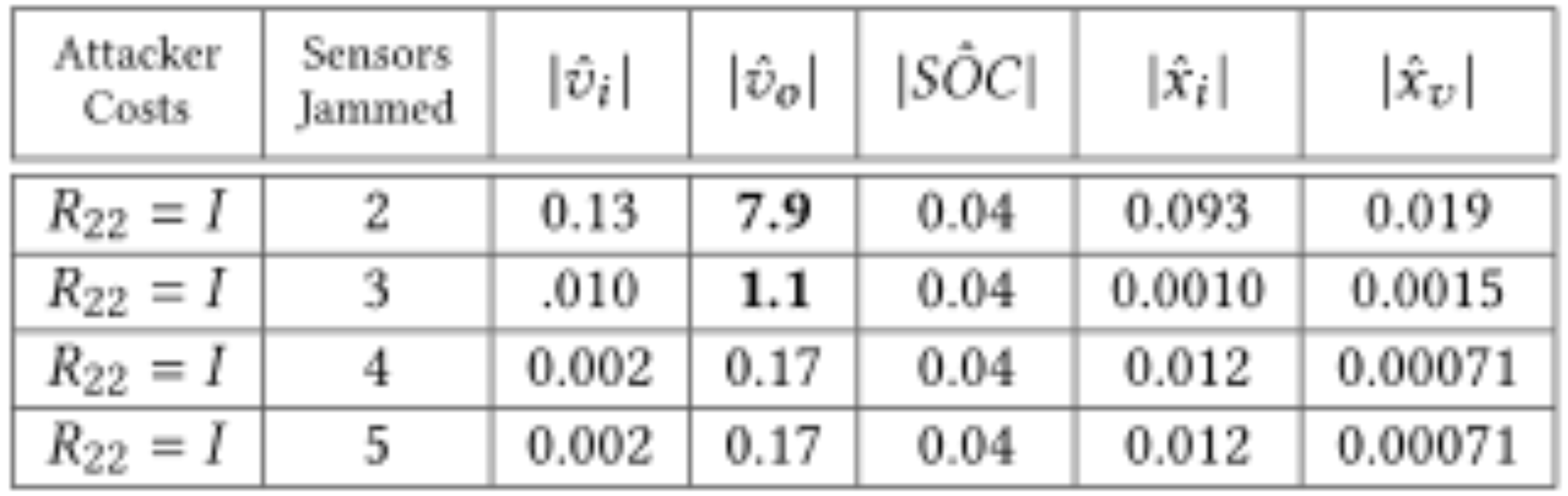
GOAL: (G0) Cause the battery to exceed the electric motor circuit temperature limit (80 C)

AND G1. Transmit CAN messages with spurious coolant temperature to prevent increase in coolant flow (@ 35 C) or initiate shutdown procedure (@ 80 C) from ECU1

OR 1. Alter MESSAGE1 from ECU2 to ECU1 that conveys coolant temp information such that the readings are below 80 C and within expected typical ranges.

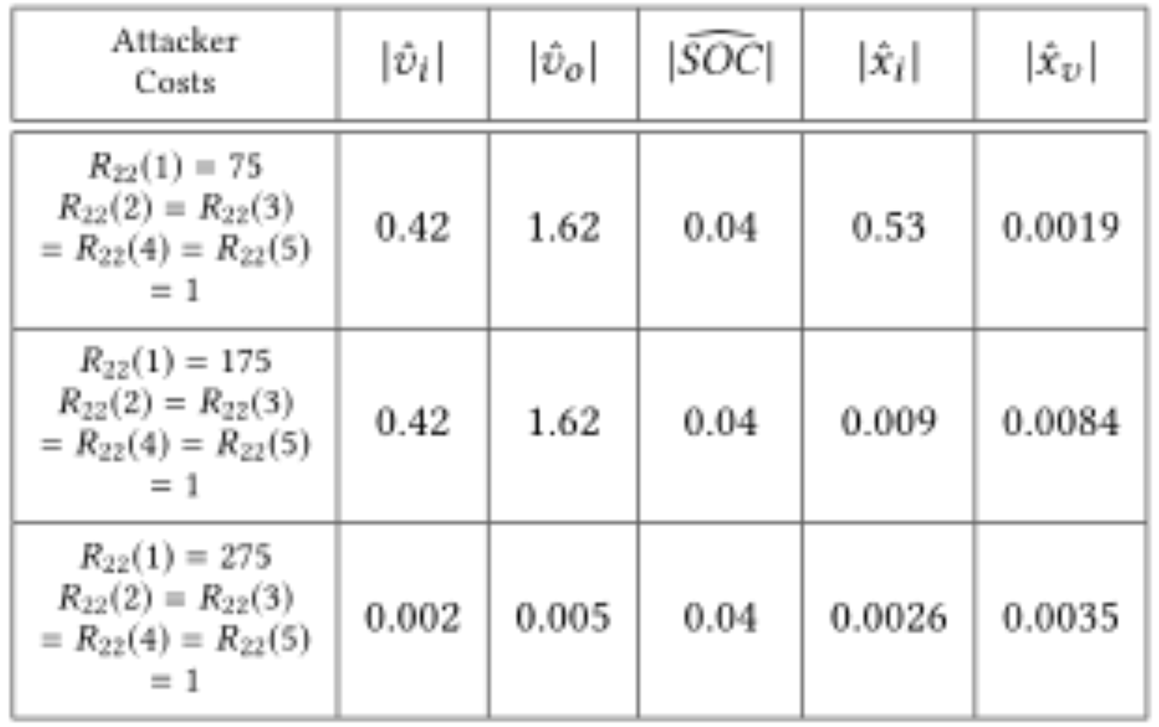
Technical Accomplishments and Progress: T3

- **Trust Models of BEV**
  - Attack vectors: jamming, false-data injection, false-actuation injection
  - Initial system: BMS (DC/DC converter, linearized)
  - Game theoretic formulation that allows for
    - cost-benefit analysis of attacks and defenses
  - Extensions: differing rationalities/capabilities/knowledge; attack outcomes generalized: loss of controllability, stability, observability
  - Deliverable: *Linear-Quadratic Game Theoretic Analysis for Securing Battery Management Power Converter Systems*, ACM AutoSec, 2020
  - Insight: Jamming: lowest cost and most effective attack leading to instability; redundancy necessary in future design



Attacker Costs	Sensors Jammed	$\lvert\hat{v}_i\rvert$	$\lvert\hat{v}_o\rvert$	$\lvert\hat{SOC}\rvert$	$\lvert\hat{x}_i\rvert$	$\lvert\hat{x}_v\rvert$
$R_{22} = I$	2	0.13	**7.9**	0.04	0.093	0.019
$R_{22} = I$	3	.010	**1.1**	0.04	0.0010	0.0015
$R_{22} = I$	4	0.002	0.17	0.04	0.012	0.00071
$R_{22} = I$	5	0.002	0.17	0.04	0.012	0.00071

Table 2: State perturbation of values while one sensor is being jammed/FDI, with no FDA and without additional defense. The values in bold show significant output voltage perturbation based on the attack. It can be seen that the current sensor is most vulnerable to attack, followed by the voltage sensor.

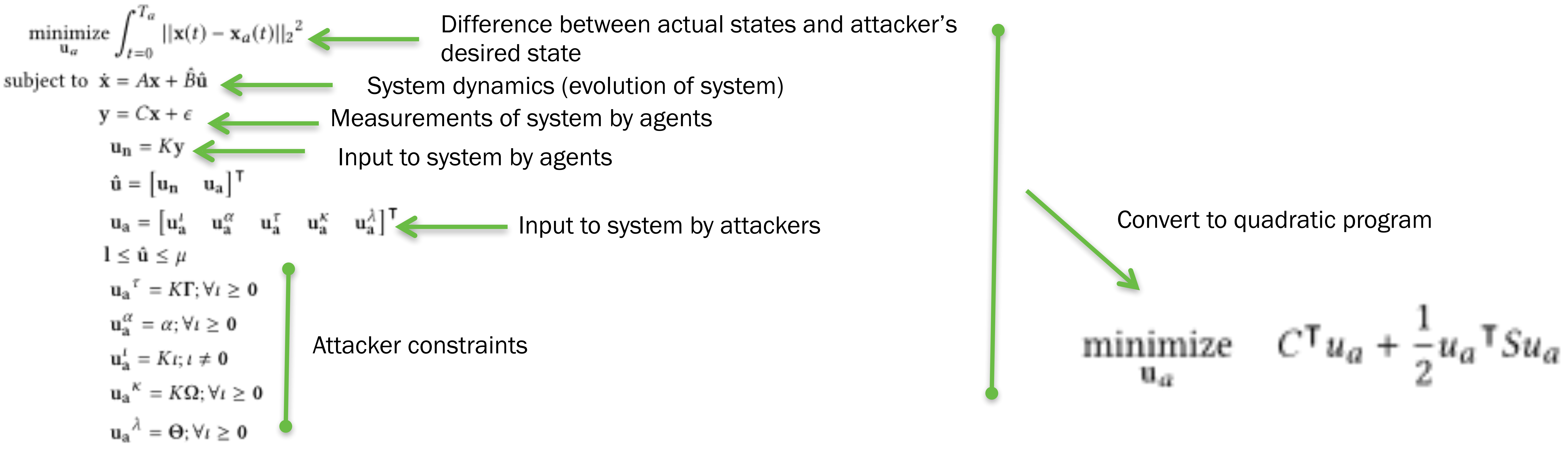


Attacker Costs	$\lvert\hat{v}_i\rvert$	$\lvert\hat{v}_o\rvert$	$\lvert\widehat{SOC}\rvert$	$\lvert\hat{x}_i\rvert$	$\lvert\hat{x}_v\rvert$
$R_{22}(1) = 75$ $R_{22}(2) = R_{22}(3)$ $= R_{22}(4) = R_{22}(5)$ $= 1$	0.42	1.62	0.04	0.53	0.0019
$R_{22}(1) = 175$ $R_{22}(2) = R_{22}(3)$ $= R_{22}(4) = R_{22}(5)$ $= 1$	0.42	1.62	0.04	0.009	0.0084
$R_{22}(1) = 275$ $R_{22}(2) = R_{22}(3)$ $= R_{22}(4) = R_{22}(5)$ $= 1$	0.002	0.005	0.04	0.0026	0.0035

Table 5: State perturbation values when FDA is permissible as the only method of attack. The difference between minorly and moderately reinforced FDA sensors is relatively small as they use the same equilibrium trajectory as the best case scenario, but more heavily reinforced FDA sensors have a different equilibrium as the most optimal, thereby making a larger impact.

Technical Accomplishments and Progress: T3

- **Trust Models of EVSE/BEV**
  - Attack vectors: delay, jamming, false-data injection, false-actuation injection
  - Initial system: LTI
  - Optimization problem: all attacks represented as input to system
    - Incorporate: nominal control, attack states of interest
    - Manual specification of attacker objective(s)
    - Novel attack sequences discoverable
  - Deliverable: *Towards Automatic Attack Generation for Cyber-Physical Systems*, TBD, 2020
  - Insight: Simulation framework created to evaluate designs against sensor and actuator attacks



$$\underset{\mathbf{u}_a}{\text{minimize}} \int_{t=0}^{T_a} ||\mathbf{x}(t) - \mathbf{x}_a(t)||_2{}^2$$

Difference between actual states and attacker's desired state

$$\text{subject to } \dot{\mathbf{x}} = A\mathbf{x} + \hat{B}\hat{\mathbf{u}}$$

System dynamics (evolution of system)

$$\mathbf{y} = C\mathbf{x} + \epsilon$$

Measurements of system by agents

$$\mathbf{u_n} = K\mathbf{y}$$

Input to system by agents

$$\hat{\mathbf{u}} = \begin{bmatrix} \mathbf{u_n} & \mathbf{u_a} \end{bmatrix}^\intercal$$

$$\mathbf{u_a} = \begin{bmatrix} \mathbf{u}_\mathbf{a}^\iota & \mathbf{u}_\mathbf{a}^\alpha & \mathbf{u}_\mathbf{a}^\tau & \mathbf{u}_\mathbf{a}^\kappa & \mathbf{u}_\mathbf{a}^\lambda \end{bmatrix}^\intercal$$

Input to system by attackers

$$\mathbf{l} \leq \hat{\mathbf{u}} \leq \mu$$

$$\mathbf{u_a}{}^\tau = K\Gamma; \forall \iota \geq \mathbf{0}$$

$$\mathbf{u}_\mathbf{a}^\alpha = \alpha; \forall \iota \geq \mathbf{0}$$

$$\mathbf{u}_\mathbf{a}^\iota = K\iota; \iota \neq \mathbf{0}$$

$$\mathbf{u_a}{}^\kappa = K\Omega; \forall \iota \geq \mathbf{0}$$

$$\mathbf{u_a}{}^\lambda = \Theta; \forall \iota \geq \mathbf{0}$$

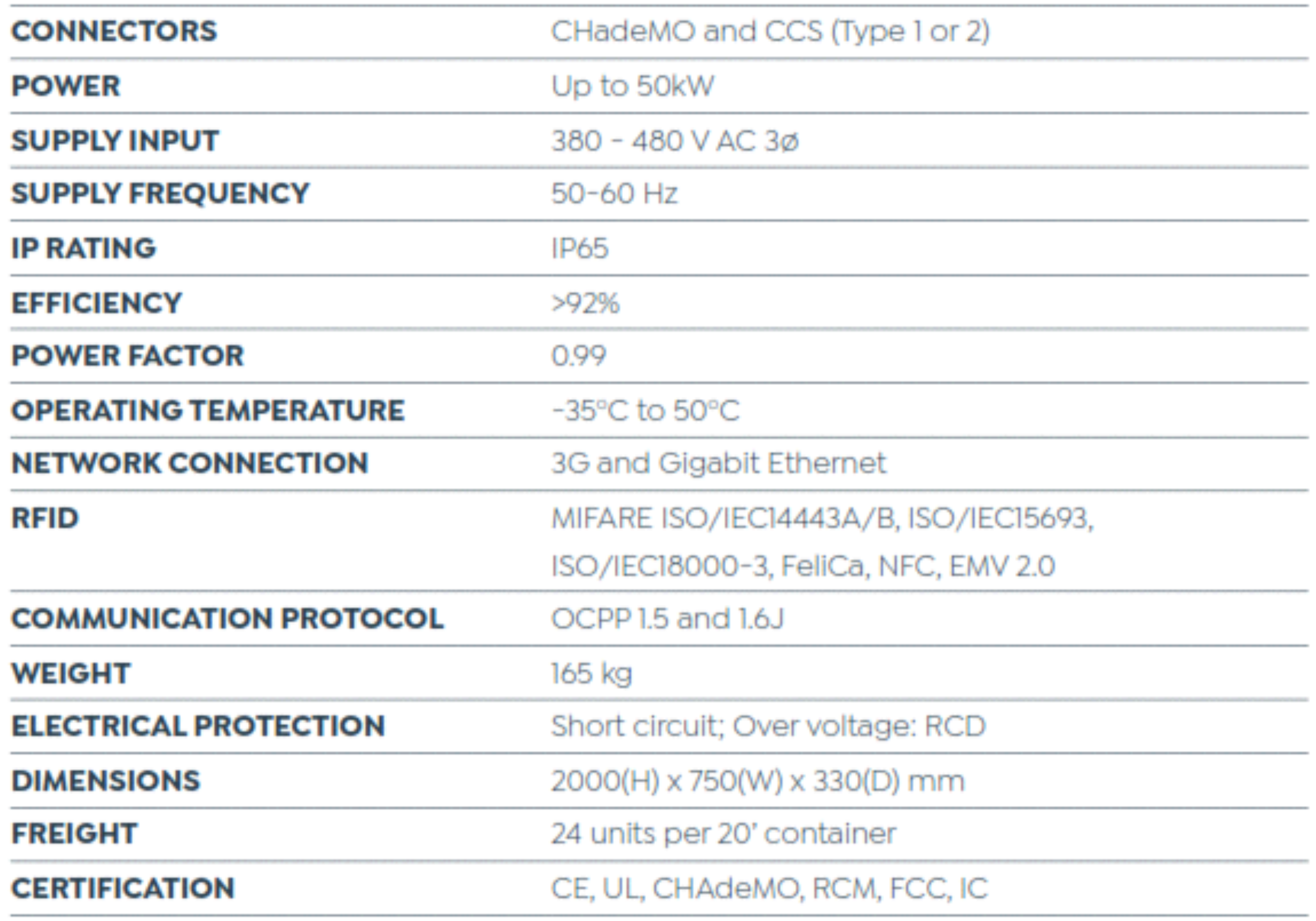
Attacker constraints

Convert to quadratic program

$$\underset{\mathbf{u}_a}{\text{minimize}} \quad C^\intercal u_a + \frac{1}{2} u_a{}^\intercal S u_a$$

Technical Accomplishments and Progress: T4,7

- **50kW DC Fast Charger and a 350kW XFC Ordered from Tritium**
  - 50 kW received in December 2019
  - 350 kW XFC estimated delivery is March-April 2020
  - Future work:
    - EVSE vulnerability assessment (T4, Q3, 2020)
    - Installation of the chargers and their integration within the HIL test environment (T7)

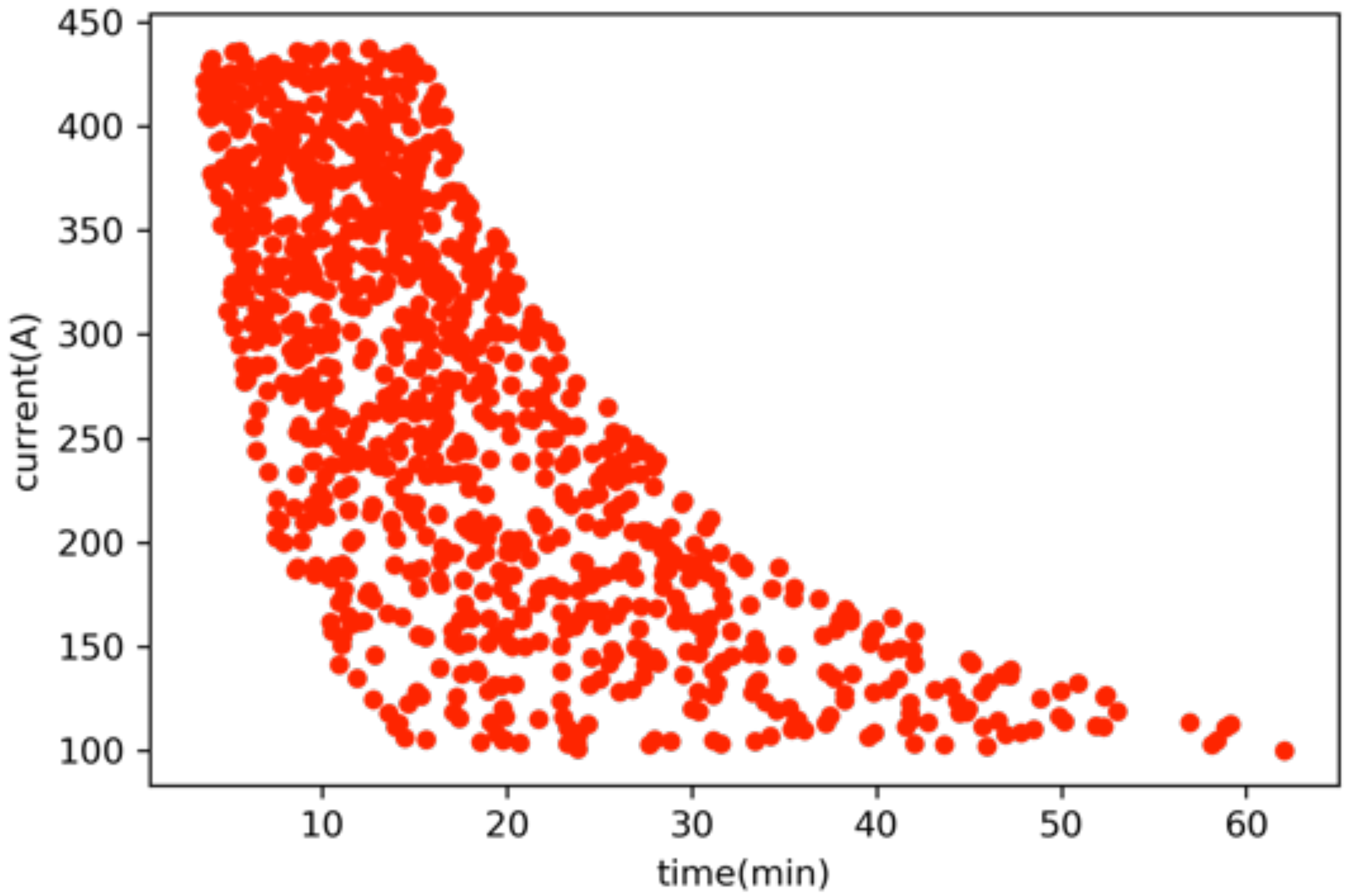


CONNECTORS	CHadeMO and CCS (Type 1 or 2)
POWER	Up to 50kW
SUPPLY INPUT	380 - 480 V AC 3ø
SUPPLY FREQUENCY	50-60 Hz
IP RATING	IP65
EFFICIENCY	>92%
POWER FACTOR	0.99
OPERATING TEMPERATURE	-35°C to 50°C
NETWORK CONNECTION	3G and Gigabit Ethernet
RFID	MIFARE ISO/IEC14443A/B, ISO/IEC15693, ISO/IEC18000-3, FeliCa, NFC, EMV 2.0
COMMUNICATION PROTOCOL	OCPP 1.5 and 1.6J
WEIGHT	165 kg
ELECTRICAL PROTECTION	Short circuit; Over voltage: RCD
DIMENSIONS	2000(H) x 750(W) x 330(D) mm
FREIGHT	24 units per 20' container
CERTIFICATION	CE, UL, CHAdeMO, RCM, FCC, IC

Technical Accomplishments and Progress: T5,6

- **Enabling Simulation/Evaluation of a Microgrid**
  - ComEd/VT has developed RSCAD model of the Bronzeville Community Microgrid (BCM)
    - 5,000 nodes, feeders, generating sources, and loads
    - RTDS/OPAL-RT HIL tests and simulation of the impact of XFC EV chargers on the BCM
      - Proof-of-concept: publicly available EV charging data
      - Charger-specific data: project partner and laboratory tests
    - Testing will be done in ComEd's Integration and Technology lab
    - Future: XFC integration and HIL test plan will be developed together with VT team; reachability analysis to evaluate attack effects/detection

ComEd Integration and Testing Laboratory



BEV Charging Profiles for EVSE Characterization

Technical Accomplishments and Progress: T8

- **Proactive and Reactive Defense Mechanism (MTD)**
  - Use of redundant sensor and actuators
    - Proactive: switch active unit(s) in unpredictable and stochastic fashion
    - Reactive: remove compromised units
    - Increases cost to attacker with minimal cost to defender
      - Sensors inexpensive: physical redundancy
      - Actuators expensive: virtual redundancy
  - Detection relies on prediction
    - Deliverable: *On the Efficacy of Model-Based Attack Detectors for Unmanned Aerial Systems*, ACM AutoSec, 2020
    - Insight: physics-based models ineffective due to process and measurement noise; learning-based, model-free approaches needed to detect attacks

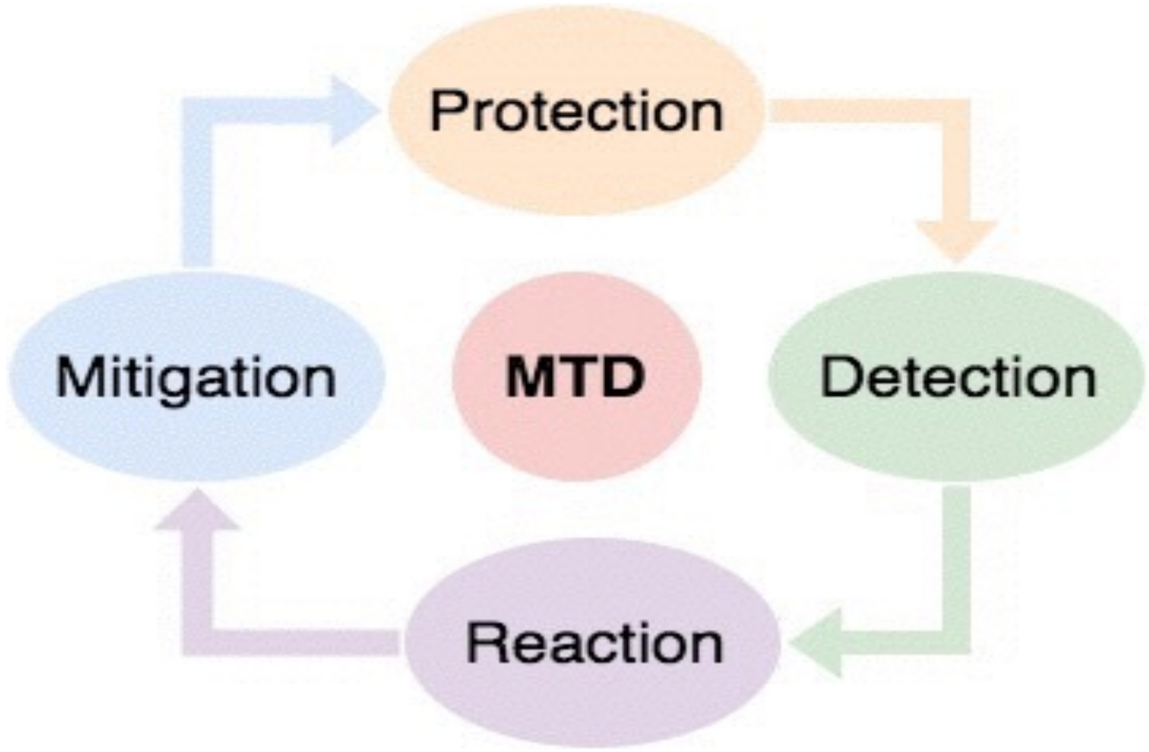
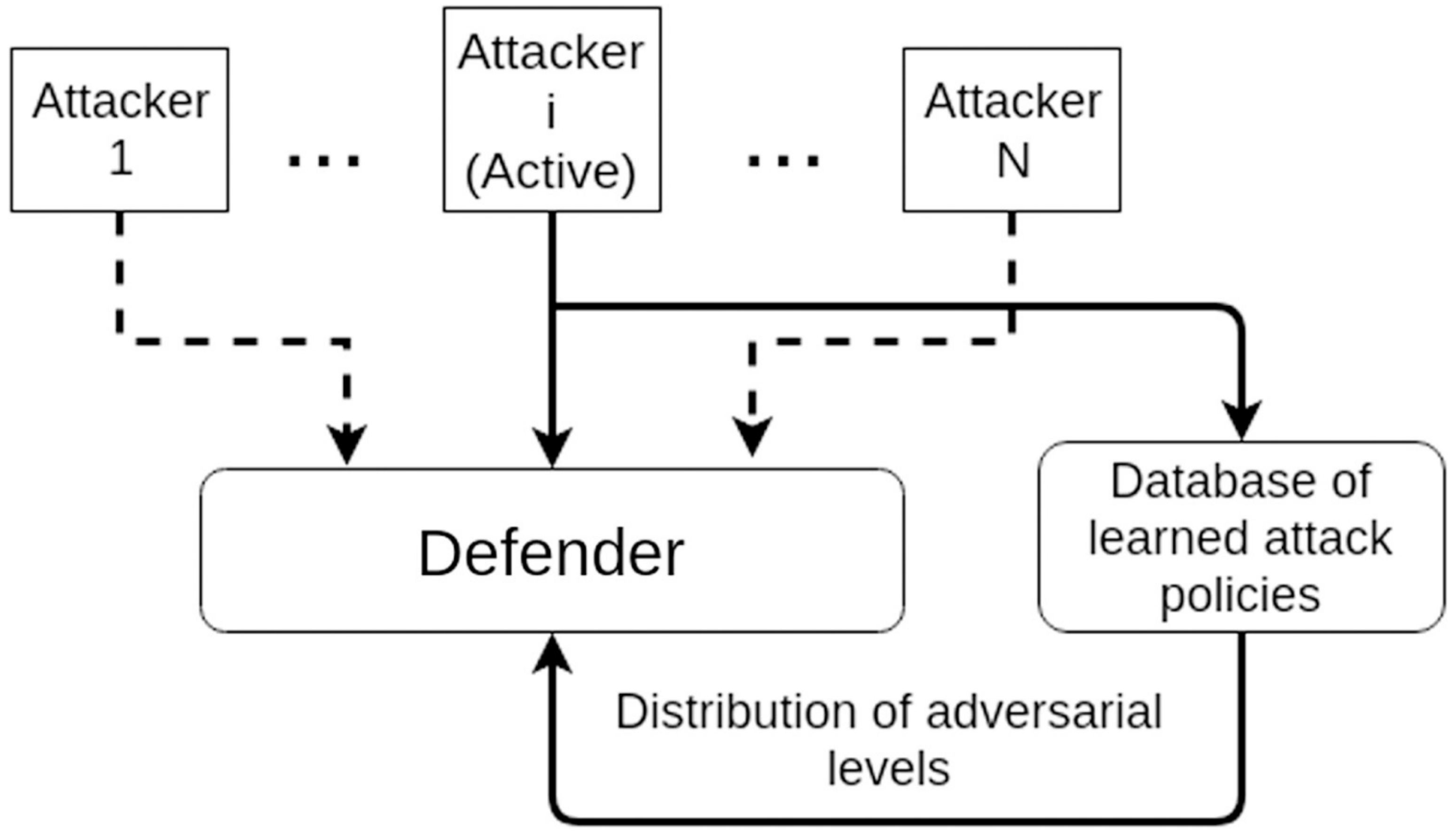


Fig. MTD framework with detection and mitigation


Attacker 1
...
Attacker i (Active)
...
Attacker N
Defender
Database of learned attack policies
Distribution of adversarial levels

Technical Accomplishments and Progress: T8

- Proactive and Reactive Defense Mechanism (MTD)
  - Combine the Approximate Dynamic Programming (ADP) with MTD
    - Model-free Bellman-based detection mechanism.
    - Propose a switching law to guarantee the stability of switched systems.
  - Cost-benefit analysis: Examine the minimum number of sensors and actuators to cost-effectively secure hardware
  - Deliverables: *Non-Equilibrium Dynamic Games and Cyber-Physical Security*, Systems and Control Letters, 2019; *A Moving Target Defense Control Framework for Cyber-Physical Systems*, IEEE Transactions on Automatic Control, 2020; *Robust Data-Based and Secure Switched Cyber-Physical Systems,* International Journal of Robust and Nonlinear Control, 2020; A Data-Based Private Learning Framework for Enhanced Security Against Replay Attacks in Cyber-Physical Systems, The International Journal of Robust and Nonlinear Control, 2020; Data-Based and Secure Switched Cyber-Physical Systems, IEEE Transactions on Industrial Electronics, 2020
  - Insights:
    - Learn the best defending strategy in the presence of worst case disturbances, stochastic noises, and replay attacks
    - Sensor and actuator attacks: reactive and proactive defense necessary to counter attacks
    - Proof-of-concept via simulation of moving-target defense

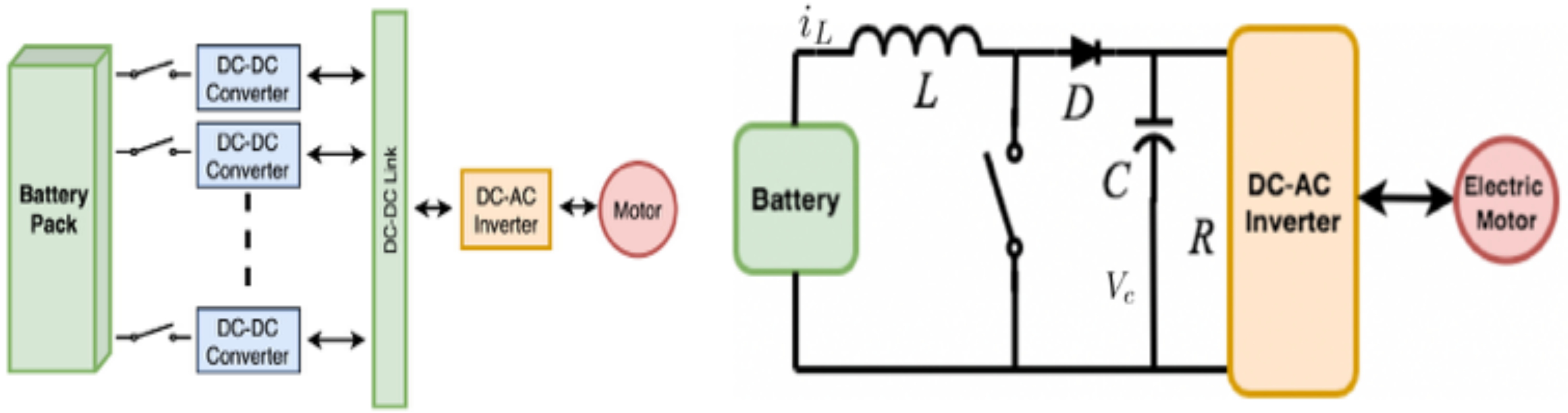
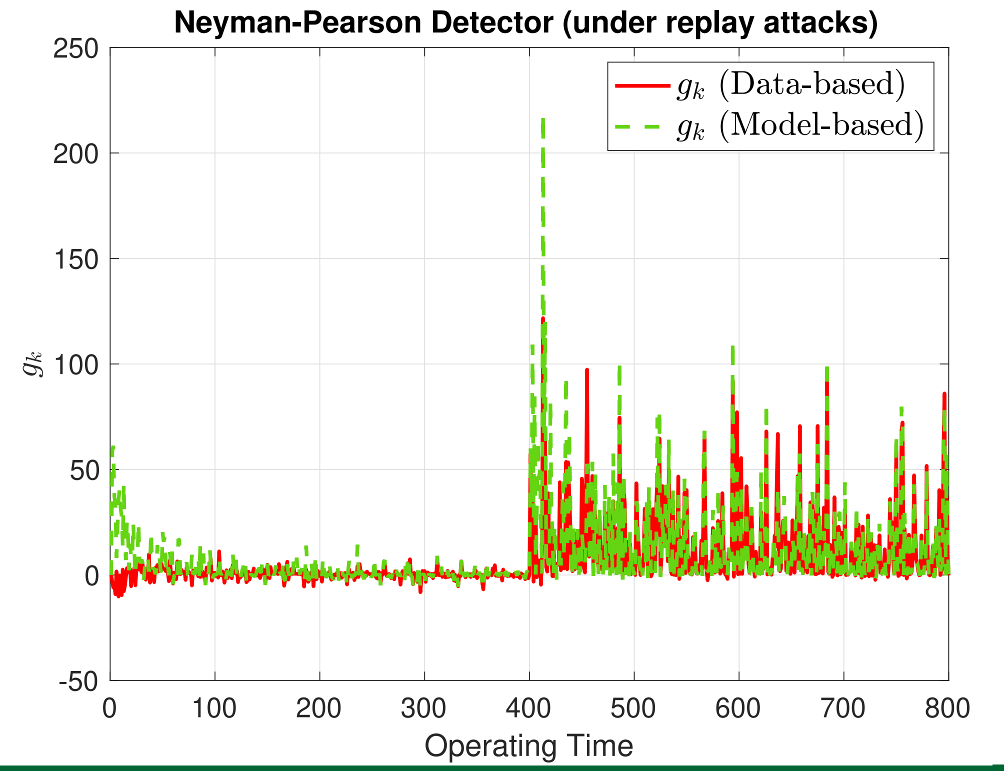
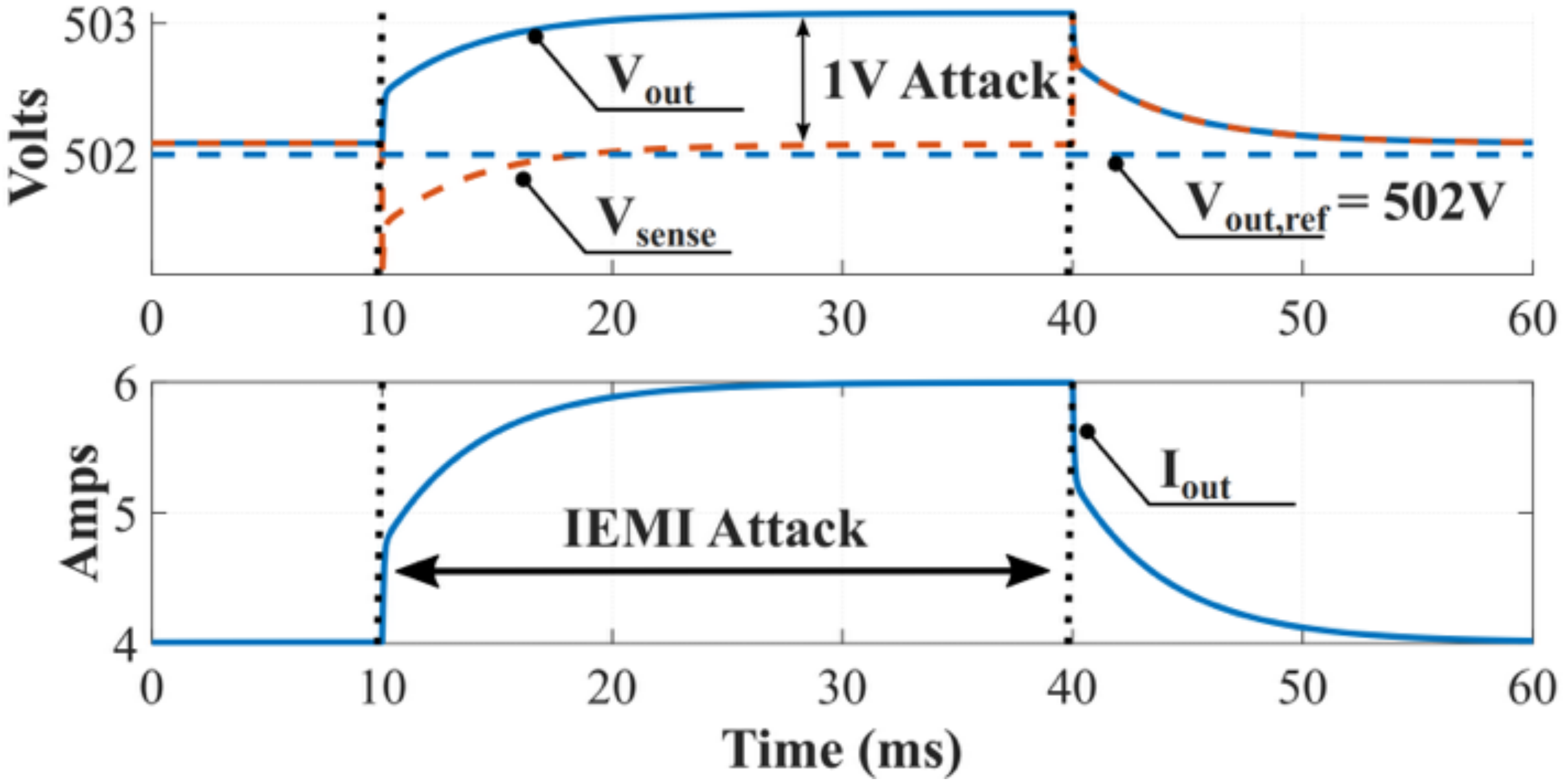


Fig. DC-DC converter topology and set-up

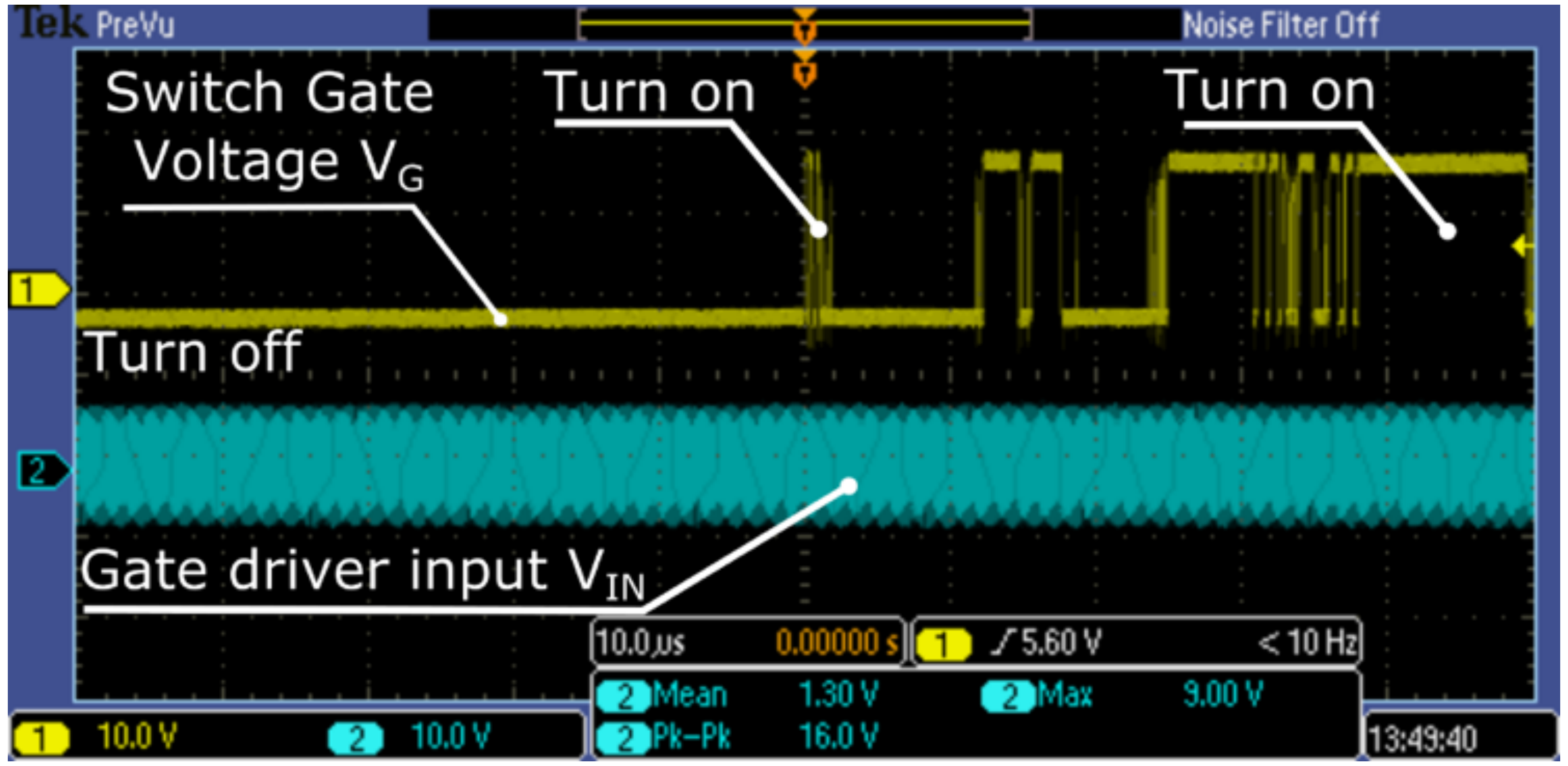


Technical Accomplishments and Progress: T9–11

- Critical Design Review
  - First-ever CPS vulnerability assessment of power converters
    - Both sensing signal and actuator signal can be attacked
    - Impact the converter output regulation and safe operation
    - Tests stopped: need test points to monitor attack effects
  - Evaluation of hardware and software mitigations; design changes
    - Invited talk: IEEE ECCE, CyberPELS, 2019
  - Deliverable: *Vulnerability assessment of XFC Power Converters*, IEEE SafeThings, 2020
  - Insights: Converters can be controlled remotely via EMI: hardware mitigations necessary



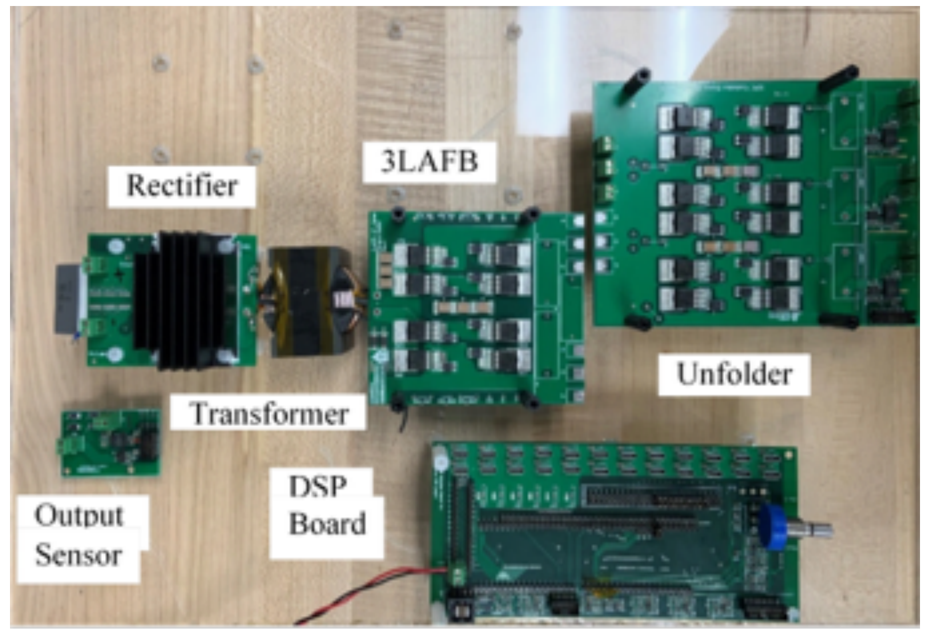
Effects of Attack



Demonstration of Gate Control via EMI

Technical Accomplishments and Progress: T9–11

- Prototype Hardware
  - 2 kW AC/DC and 30 W DC/DC
  - Incorporate mitigations: hardware, software, control (MTD)
    - Evaluate for efficacy and cost-effectiveness
    - Recommended changes to design process for security
  - Deliverables: *3-Level Asymmetric Full-Bridge Soft-Switched PWM Converter for 3-Phase Unfolding Based Battery Charger Topology, IEEE Energy Conversion Congress and Exposition*, 2019; *Cyber-Physical Security Hardened Converter Designs*, IEEE Power Electronics, 2020; *Control of the proposed XFC topology*, ECCE, 2020
- Cyber-Physical Hardened Designs
  - 480 V 3-phase ac input, 350 kW rated power XFC using 5 modules with 70 kW rated power each
  - Designed a 36.4 kWh battery pack using 55 Ah LTO cells
  - Developed a 300 W DC-DC converter prototype for the BMS
  - Extensions:
    - moving target defense for resiliency (attacker cannot know sensors or actuators used to control converters)
    - hardware mitigations (attacker cannot couple to converters so cannot influence sensors or actuators
    - cyber mitigations (communications between sensors and controller are authenticated)

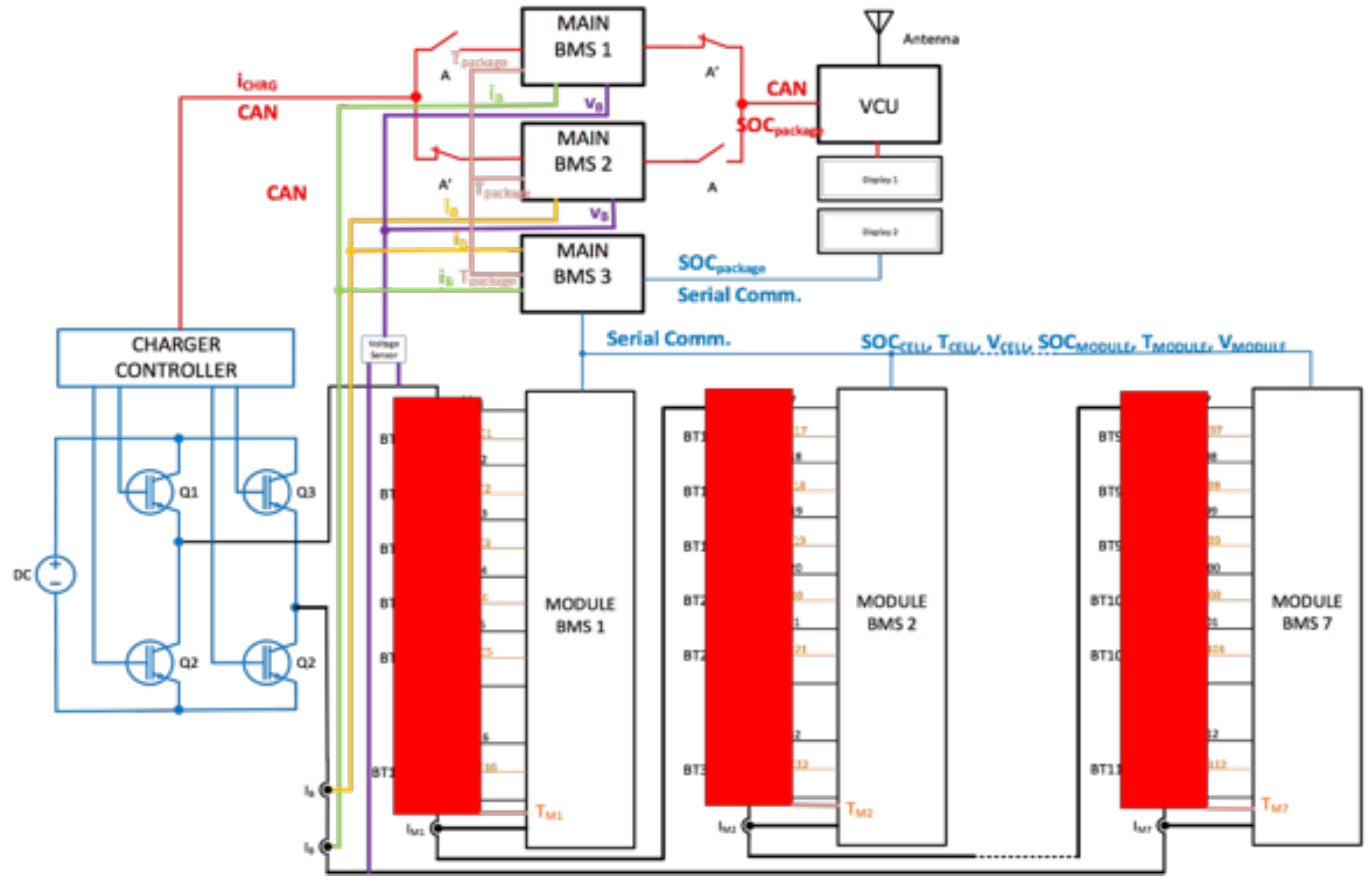


AC/DC Converter

DC/DC Converter

Technical Accomplishments and Progress: T9–11

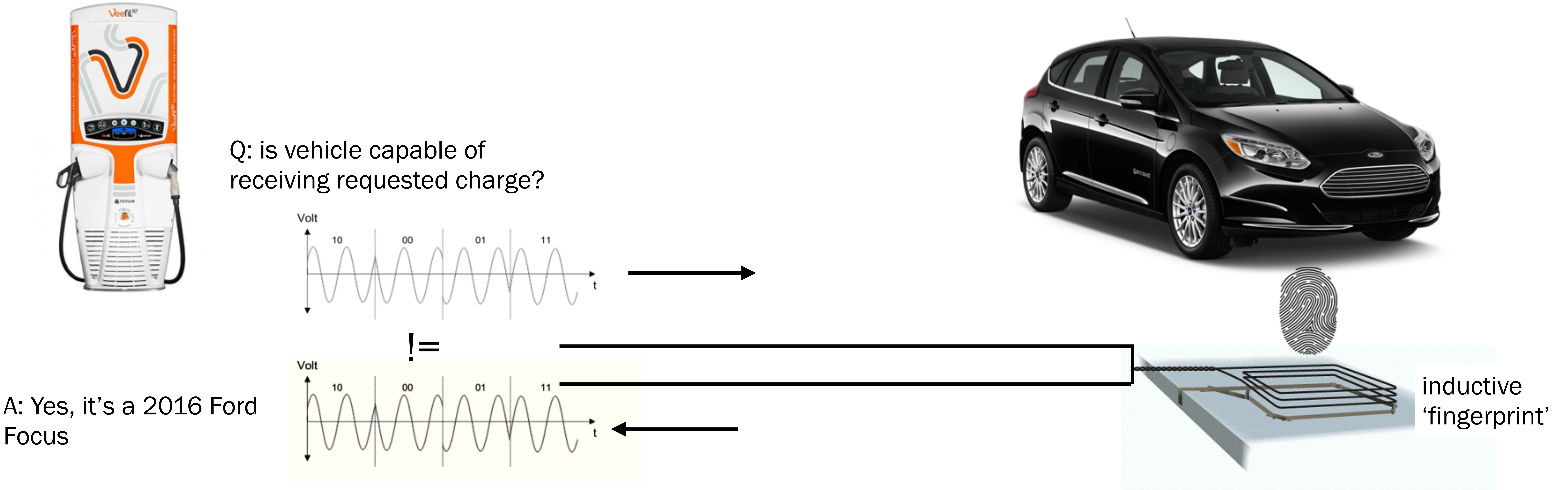
- International Collaboration
  - Modeling and validation of a 16 cell Li-Ion NMC battery system
  - Evaluation of MTD strategies (controller architectures)
  - ANN based SOC estimation and observer schemes
    - Estimate all battery parameters on-line
    - Eliminates parameter tables (aid in optimization)
  - Publications: *MTD-based Novel Strategies for Secure BMS and Fast Charging Systems*, ITEC, 2020; *SOC estimation for BEV Batteries using ANN*, ITEC, 2020; *Data-Based Modeling and SOC Estimation for Li-Ion Batteries in EV*, IEEE ISIE, 2020.



General Schematic for MTD based Secure BMS-XFC Concept

Technical Accomplishments and Progress: T12

- Inductive Fingerprinting
  - RFID-inspired (car is `RFID tag’)
  - No fundamental changes to inductive-loop systems
    - Existing approaches (e.g., Colpitts oscillator) discriminate between vehicle types
    - Our approach: complex, wide-band signalling
  - Goal: discriminate between same-model vehicles
    - Validate using real-world data



Q: is vehicle capable of receiving requested charge?

A: Yes, it’s a 2016 Ford Focus

inductive ‘fingerprint’

Technical Accomplishments and Progress: T13

- Formally-Verified Firmware Update Procedure
  - Runs in Trusted Execution Environment
    - Guaranteed to execute
    - Cannot be modified
  - UPTANE-compatible
  - Components and toolchain selected
  - Porting Python to C code for verification
  - Support from new project partner

Responses to Previous Year Reviewers' Comments

- *A possible concern is the use of an older BEV that may not have the most up-to-date software, but this may not be a major concern as the focus here is on EVSE.*
  - Architectural analysis of vehicle indicated several possible attack points; three-level remediation in new designs: control, cyber-physical, and cyber
- *The reviewer stated that it appears this project is somewhat behind schedule. No milestone schedule was provided.*
  - At roughly 50% project is now on schedule and milestone schedule provided
- *The project started in October 2018 and ends December 2020. It is only 20% completed, when it should be closer to being 30% completed.*
  - Contracting, partner changes, and COVID-related manufacturing halts have resulted in delay; six month no-cost extension filed for year one budget period
- *[C]ollaborate, with DHS and DOT to ensure there is no duplication in protection … or interference*
  - Gave presentation at NIST-hosted 'Federal Research in EVSE Cybersecurity'

Responses to Previous Year Reviewers' Comments

- *The reviewer believed that this is an aggressive project with many goals. It may be difficult to accomplish everything that is planned.*
  - We concur in the aggressive nature of project goals but believe that we have assembled the right team to accomplish them

Collaboration and Coordination

- **Interactions**
  - Prime call w/DOE PM: monthly (phone)
  - Prime call w/all partners: monthly (videoconference)
  - Prime call w/individual partners: monthly (videoconference)

	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15
VT	*S*	*S*	*L*	*S*	*S*	*S*	*L*	*S*	*S*			*L*	*L*	*S*	*S*
GT			*S*					*L*	*S*						
USU									*L*	*L*	*L*	*S*			
TRI			*S*	*S*					*S*				*S*	*S*	
CEC			*S*		*L*	*L*	*S*								
FMC		*S*	*S*												
GE	*L*	*L*	*S*	*L*					*S*			*S*	*S*	*L*	*L*

(L)ead, (S)upport

Each sub-task averages 2.67 partners in participation

Remaining Challenges and Barriers

- **Barriers and Roadblocks**
  - – Delays due to XFC EVSE availability
  - – COVID-19 has resulted in lab shutdowns for VT and travel bans for VT and GE until Jun 10th, 2020
    - – BEV and EVSE assessments delayed until Q3
    - – USU may also experience delays (BMS, AC-DC converter) due to COVID-19
- **Disparate knowledge/simulation domains across teams**
- **Physical realization of countermeasures**
  - – Generic cyber-physical systems provably secure (against known attacks)
  - – Implementations are flawed
    - Design of redundant /diverse sensing regimes not vulnerable to common (same) attacks
    - Cost-effective and resilient parallel actuation strategies
    - Redundancy/diversity leading to exponential gains in security (commonly only linear)

Proposed Future Research

Milestone #	Task	Milestone
3 (Q3&4 2020)	*Trust Models (VT lead, GT, GE, Tritium, Ford, ComEd support)*	*Comprehensive list of attack points and the utility of attacking/defending them.*
4 (Q3, 2020)	*Vulnerability Assessment of EVSE (GE lead, VT and Tritium support) [Q3, 2020]*	*Attack trees and attack graphs that indicate likely compromise points and the attack sequence necessary to achieve attacker goals.*
7 (Q3, 2020)	*Create BEV charging profiles using Monte Carlo simulation and insert BEV charging units with variation of charging profiles into the microgrid (VT*	*Different BEV charge profiles are created based on real-world data*
8 (Q2, 2020)	*Combined proactive and reactive defense mechanism (GT lead, VT support)*	*A proactive and reactive defense framework for the EVSE/BEV/grid controllers.*
9 (Q2, 2020)	*Iterative design of 300 kW AC-DC converter and 5 kW integrated active BMS plus DC-DC converter (USU lead, VT, GT, OBS, and Tritium support)*	*Critical design review completed with team and program manager approval of hardened designs.*
10 (Q2, 2020)	*Hardware construction of BMS with integrated 5 kW DC-DC for vehicle LV loads (USU lead)*	*Hardware demonstration with functional operation of modified battery pack, BMS, and DC-DC and*
11 (Q2, 2020)	*Hardware construction of 60 kW module prototype for AC-DC converter (USU lead)*	*Hardware demonstration with functional operation of the 60 kW module with verified*

Any proposed future work is subject to change based on funding levels.

Proposed Future Research

Milestone #	Task	Milestone
12 (Q3, 2020)	*Devising device fingerprinting methodologies for conductive and inductive chargers*	*EVSE capable of securely determining presence and type of vehicle*
13 (Q3, 2020)	*Creation of formally verified update procedure (GE/ VT Co-lead and Tritium support)*	*A TCB-based routine capable of initiating remote update procedure, authenticating firmware, and installing it.*
14 (Q2, 2021)	*Allowing updates to EVSE when primary communication channel is disabled (GE lead, VT and Tritium support)*	*Proof-of-concept demonstration that update routine can fall-back to secondary communication channel.*
15 (Q4, 2020)	*Privacy of EVSE-BEV, EVSE-Grid communication (GE lead, VT support)*	*Privacy Impact Assessment of EVSE/ BEV communication: The PIA analyzes the data flows to identify personally identifiable information. Data collection, retention, use, disclosure are then analyzed to ensure appropriate privacy controls.*

Any proposed future work is subject to change based on funding levels.

Summary

- **Goal: secure and efficient charging**
- **Approach: hardware/software-security (HW/SW-Sec) co-design**
  - Develop security-hardened controllers, converters, and monitoring systems for XFC
    - maintain user privacy
    - secure sensing and actuation techniques
    - learning-enabled moving-target defense
    - remediation of vulnerabilities through remote updates
  - Benefits
    - Minimizing (secure) design time of future systems
    - Address findings of vulnerability assessments
    - Critical infrastructure that can resist (as a function of cost), and be resilient to, attack
  - The feasibility demonstrated on a real-world testbed that includes an XFC unit and BEV situated in a microgrid
  - Multi-disciplinary team and industry-academic partnership
    - Unique perspectives and expertise to examine threats and solutions